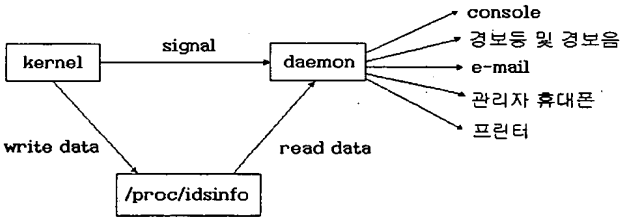
KOREAN PATENT ABSTRACTS(KR)

Document Code:A
(11) Publication No.1020020091340 (43) Publication.Date. 20021206
(21) Application No.1020010029899 (22) Application Date. 20010530
(51) IPC Code:
G06F 15/00

(71) Applicant:
NA, IN SIK
(72) Inventor:
LEE, BYEONG DO
LEE, MYEONG HO
NA, IN SIK
PARK, JANG SU
(30) Priority:

(54) Title of Invention
SYSTEM FOR DETECTING INVASION IN REAL TIME ON LINUX KERNEL

Representative drawing



(57) Abstract:

PURPOSE: A system for detecting invasion is provided to develop a demon program for performing an evaluation of a legality of an operation and a position of an operator on a network, a right of an operator, etc. for detecting an invasion with respect to a computer system in real time.

CONSTITUTION: When a processor is started, a process ID, a command, a log-in name, a remote host IP, a Set-user-ID, a Set-group-ID, etc. are obtained by inserting a code in a search_binary_handler function. If a program is started, a do_execve function is called for creating a processor. The do_execve function calls a search_binary_handler for searching a program handler adapted to a format of the program. It is checked whether a root right which is an effective user ID is possessed in a search_binary_handler module. If the processor has a root right, a log-in name which is an operator account is obtained in an environment variable of the processor. A remote host IP which displays a position of a remote connected person is obtained. A signal is transmitted to a demon. A kernel checks whether a security demon is operated continuously whenever a program is started. The search_binary_handler module is returned to a do_execve. The information is transmitted to the demon through a virtual file of an idsinfo in a proc file system by a get_idsinfo code. Necessary additional codes are as follows. A file as an idsinfo file is defined in a proc_dir_entry structure. The idsinfo file is registered in the proc file system using a proc_register function. A get_idsinfo which having processor information in a /proc/idsinfo file is defined. If the demon reads the idsinfo file, a get_root_array function calls a get_idsinfo.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.		(11) 공개번호	특2002-0091340
G06F 15/00		(43) 공개일자	2002년12월06일
(21) 출원번호	10-2001-0029899		
(22) 출원일자	2001년05월30일		

(71) 출원인 라인식
대한민국
121-781
서울 마포구 성산2동 시영아파트 22-1405호

(72) 발명자 라인식
대한민국
121-781
서울 마포구 성산2동 시영아파트 22-1405호

이명호
대한민국
361300
충청북도 청주시 흥덕구 봉명동 1603 신라아파트 2-503호

박장수
대한민국
138913
서울특별시 송파구 장실2동 주공아파트 278-508

이병도
대한민국
361270
충청북도 청주시 흥덕구 복대동 삼일아파트 107-1302

(77) 심사청구 있음

(54) 출원명 리눅스 커널 기반의 실시간 침입탐지 시스템

요약

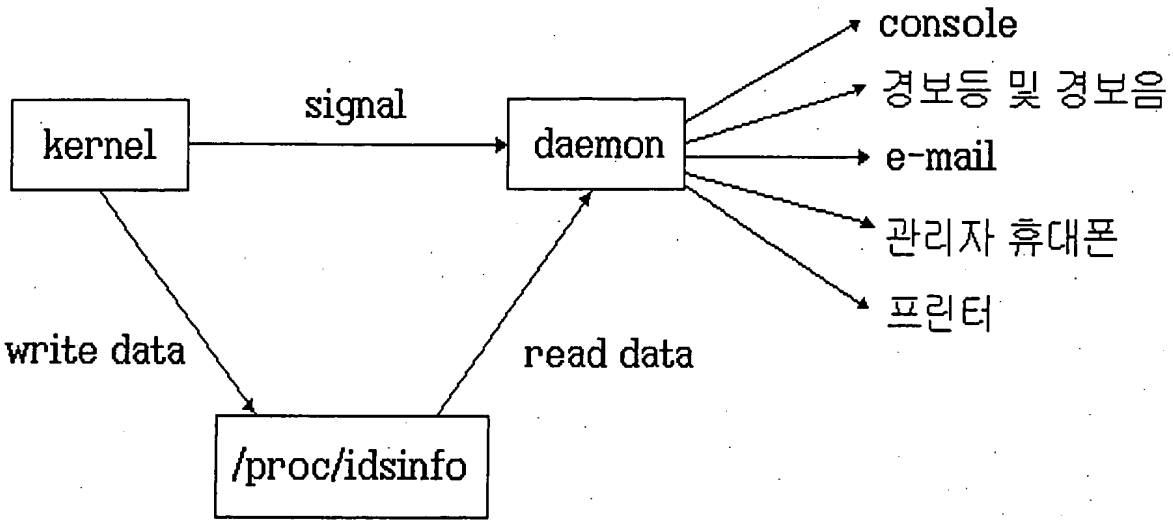
본 발명은 컴퓨터 시스템에 대한 침해를 실시간으로 탐지하는 새로운 기술로서 컴퓨터 운영시스템의 최하위 레벨인 커널에서 수행되는 침입탐지 시스템이다.

이를 위하여 본 발명은 컴퓨터 프로그램이 수행되는 시점에서 작업환경에 대한 정보를 획득하여 저장하도록 커널을 수정하였다. 이렇게 보고된 정보는 일종의 감시 프로그램인 데몬(daemon) 프로그램에 의하여 작업을 수행시킨 사용자의 위치, 프로그램의 수행계통, 작업의 적법성 유무를 판단하게되며 결과를 시스템 단말기인 콘솔(console)과 침입감시제어장치, 전자우편, 관리자 휴대폰 등으로 알린다.

기존의 네트웍 기반이나 호스트 기반의 침입탐지 시스템들의 침입 탐지율이 50%를 넘지 못하고 시간이 경과함에 따라 오히려 떨어지는 단점이 있을 뿐만 아니라 이를 우회하는 방법도 소개되어 있어 침입탐지의 실효성은 날로 감소되는 추세이다.

반면 본 발명은 컴퓨터에서 수행되는 작업에 대한 직접 추적을 통해 우회 가능성을 배제함으로써 거의 모든 침입을 탐지할 뿐만 아니라 관리자의 허가 없는 작업명령이 수행되는 것을 방지하고 해커들의 침입흔적 은폐 및 삭제를 원천적으로 봉쇄할 수 있는 새로운 발명이다.

대표도



색인어

커널, root, 프로세서, signal, 사용자IP, IP, 해킹, 로깅, proc, 경광등, 경보벨, 침입감시제어장치, 이메일, 핸드폰, 문자전송, 리눅스, 서버, 추적

경세서

도면의 간단한 설명

도1]은 대표도이며 본 발명의 전체 흐름을 표시한 것이다

도2]은 커널내에서 프로세서의 정보를 획득하는 코드의 플로우 챠트이다. 1) search_binary_handler 함수내에서 effective user ID가 root권한을 가지고 있는지 확인한다.

2) 루트권한을 가진 프로세서라면 프로세서의 환경변수에서 logname을 획득한다.

3) 4) 에 의해 remote host IP를 획득한다.

5) 데몬에 시그널을 보낸다.

6) 커널은 보안데몬이 동작하고 있는지 프로그램이 기동할때마다 계속 확인한다.

이후, search_binary_handler 함수는 do_execve로 복귀한다.

도3]은 침입감시 제어장치로써 서버와 연결되어 침입 발견시 자동으로 경광등 점등 및 경보벨을 울려주는 장치이다

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명의 기술은 목적상 리눅스 운영체제를 사용하는 컴퓨터 시스템의 보안기술이고 목적을 달성하기 위한 방법상 운영체제의 핵심인 커널을 수정하고 이를 뒷받침하는 감시 프로그래인 데몬 프로그램을 새로이 작성하는 운영체제 기술이다.

종래의 컴퓨터 보안기술은 침입탐지와 침입차단으로 구분되며 다시 네트웍을 기반으로 하는 기술과 호스트(컴퓨터)를 기반으로 하는 기술로 나뉘어 진다. 하지만 이러한 종래의 기술은 다음과 같은 이유로 목적한 바를 완벽하게 이루지 못하고 있다.

) 기존의 보안 시스템은 컴퓨터 시스템 침입자들의 예상경로 몇 가지 만을 감시한다, 침입자는 다양한 침입경로를 이용하며 감시경로를 우회할 수 있다.

) 침입상태에 대한 보고가 관리자 입장에서 효과적이지 못하다. 즉, 관리자가 수시로 확인하지 않는 한 감지된 침입에 대해서도 알수가 없다.

) 컴퓨터 시스템 접근에 성공한 침입자는 자신의 침입흔적을 지워 차후 추적을 불가능하게 만들며 시스템의 복구를 어렵도록 한다.

4) 현재 시중에서 판매되는 침입탐지 시스템은 그 탐지율이 50% 이하이고 시간이 경과하면 새로운 침입 기법에 대하여 프로그램을 개정하여야 한다.

이러한 이유로 종래의 침입탐지 기술은 그 탐지율이 50%를 넘어서지 못하고 있으며 침입탐지 시스템의 평가가 50%를 기준으로 우수제품과 보통제품으로 구분되고 있는 형편이다.

발명이 이루고자 하는 기술적 과제

기존의 침입탐지 시스템이 상기와 같은 문제를 안고 있는 것은 침입자가 컴퓨터 시스템에 접근하여 작업을 수행하는 침입자의 유일한 경로를 파악하고 있지 못하기 때문이며 본 발명에서는 이러한 점에 착안하여 컴퓨터 시스템에서 모든 작업이 수행되기 위한 유일한 절차를 찾아내었고 이곳에서 작업수행과 관련한 정보들을 수집할 수 있도록 커널을 새로이 작성하였다.

이와 같이 획득된 정보를 바탕으로 수행되는 작업의 적법성과 작업자의 네트웍상의 위치, 작업자의 수행권한 등을 평가하여야 하는데 본 발명에서는 이와 같은 역할을 수행하는 데몬 프로그램을 개발하여 간단한 방법으로 효과적인 침입탐지를 수행토록 하였다.

아울러 탐지된 침입을 관리자에게 효과적으로 알리기 위하여 침입감시제어장치와 전자우편 자동전송 프로그램, 휴대폰 호출등의 프로그램을 부가하여 관리자가 적시에 대응토록 하였으며 침입자의 흔적 지우기나 사실 부인을 막기 위한 침입기록 출력시스템을 부가하였다.

본 발명으로 인한 부수 효과로 기존의 침입탐지 시스템이 침입을 탐지만 하고 차단하지 못하는 단점을 개선한 자동 차단 기능까지 보유하게 되었다.

실시간 감시는 커널 단계에서 하는 것이 가장 효과적이다. 또한 감시 데몬이 주기적으로 프로세서를 확인하는 것은 시스템에 부하를 주지만 프로세서 기동을 확인하는 커널감시는 수행률(Performance)에 거의 영향을 미치지 않는다.

커널 감시는 발생하는 모든 프로세서의 기동을 감시한다. 침입자에 의한 쉘획득후 쉘을 포함한 프로그램들의 기동에 대해 실시간으로 관리자에게 상황을 알려줄 수 있어야 한다.

발명의 구성 및 작용

커널의 search_binary_handler 함수에 [도1] 과 같이 코드를 삽입함으로써 프로세서가 기동시 process ID, command, logname, remote host IP, Set-user-ID, Set-group-ID 등을 알 수 있다.

프로그램이 기동하면 프로세서를 생성하기 위해 do_execve 함수가 호출되는데, do_execve 함수는 프로그램의 포맷에 맞는 프로그램 핸들러를 찾기 위해 search_binary_handler 함수를 호출한다. 프로세서의 정보를 확인하기 위해 추가된 코드의 진행은 [도2]이며 기능설명은 다음과 같다.

1) search_binary_handler 모듈에서 실효 사용권한이 시스템 최고권한인 (effective user ID가) root 권한을 가지고 있는지 확인한다.

2) root 권한을 가진 프로세서라면 프로세서의 환경변수에서 작업자 계정인 logname을 획득한다.

3) 4) 에 의해 원격 접속자의 위치를 나타내주는 remote host IP를 획득한다.

5) 데몬에 신호을 보낸다.

6) 커널은 보안데몬이 동작하고 있는지 프로그램이 기동할 때마다 계속 확인한다.

이후, search_binary_handler 모듈은 do_execve로 복귀한다.

이렇게 알아낸 정보는 get_idsinfo 코드에 의해 proc 파일시스템에 idsinfo 라는 가상파일을 통해 데몬에 전달된다. 이것을 위해 필요한 커널내 추가 코드는 다음과 같다.

1) proc_dir_entry 구조체에 idsinfo라는 파일을 정의한다.

2) proc_register함수를 사용하여 proc파일시스템에 idsinfo파일을 등록한다.

3) /proc/idsinfo 파일에 프로세서정보를 넣는 get_idsinfo를 정의한다.

4) 이후 데몬이 idsinfo 파일을 읽으려고 하면 get_root_array 함수에서 get_idsinfo를 호출하도록 한다.

커널은 정보전달을 위해 데몬에게 SIGINT 신호을 보내며, 신호를 받은 데몬은 /proc/idsinfo에서 해당정보를 읽어 침입 여부를 판단한다. 이후 데몬은 기동시 확인한 디스크내 Set-user-ID, Set-group-ID 프로세서를 제외한 모든 원거리 root 권한 프로세서의 정보를 콘솔 및 프린터로 출력하고, 이메일이나 휴대폰 문자메시지를 통해 관리자에게 알려준다. 또한 침입감시제어장치에 경광등 및 경보벨을 설치하여 관리자가 지정한 IP를 제외한 모든 root 권한 프로세서의 IP에 대해서는 동작을 하도록 함으로써, 관리자뿐만 아니라 다수의 직원들에 의해 감시가 이루어질 수 있도록 하였다

데몬에 관련된 경보기능은 다음과 같다.

1) 콘솔(console)출력

사용자의 요구사항에 따라 다양한 형태의 이벤트를 표시할 수 있다, 출력방식은 그래픽과 텍스트방식으로 표시할 수 있으며 이는 사용자의 편의성을 고려하여 표출할 수 있는 경보기능의 일부이다

2) 침입감시 제어장치

도2에 나타나 있는 것처럼 리눅스 서버의 통신포트(시리얼 또는 USB)에서 침입감시 제어장치에게 통신하게 된다, 침입감시 제어장치의 제어 신호는 특정신호를 송/수신하도록 자체적으로 OneChip CPU를 사용하여 부품의 간소화 및 효율성을 높였으며 또한 경광등 및 경보벨 제어는 CPU에서 제어하는 릴레이 1, 2의해서 제어하게 된다.

도3의 기능 설명은 리눅스 서버에 대해 해킹을 시도하면 이를 감지하여 경광등 및 경보벨으로 경보를 출력하는 방식으로 관리자가 24시간 서버 앞에서만 관리할 수가 없으므로 자리를 이동시 경보기능를 동작시키면 외부 해킹으로부터 실시간 모니터링 및 감시를 할 수 있는 체계를 구축하고자 본 발명을 하였다.

3) 이메일 전송

메일 전송 방식은 서버 관리자가 외출 및 퇴근시 비상대책의 일환으로 서버에 해킹 침투 발생시 신속하게 이메일을 전송하기 위한 제어 방식이다

제어방식은 데몬이 메일 명령어를 호출하여 서버 관리자 및 관련자의 메일 주소로 메일을 전송하게 된다

4) 관리자 휴대폰 문자메시지 전송

또한 휴대폰 전송 방식은 서버 관리자가 외출 및 퇴근시 비상대책의 일환으로 서버에 해킹 침투 발생시 신속하게 휴대폰으로 전송하기 위한 제어 방식이다

5) 데몬의 관리자모드 제어 방식

- 전체 확인모드 방식

이 방식은 모든 프로세서의 동작 상태를 상시 감시하여 정보를 전달하는 방식이다

- 자동 확인모드 방식

emote host IP를 가진 침입이라고 판단되는 프로세서의 정보만을 전달한다.

- 통과 IP 설정 방식

관리자가 외부에서 원격관리를 해야 할 경우 경보가 발생하지 않도록 하는 remote host IP를 설정할 수 있도록 한다.

발명의 효과

리눅스 시스템의 커널 단계에서의 감시에 의해 기존의 리눅스 시스템이 갖고 있는 침입확인의 어려움을 해결함으로써 관리자는 침입이 발생시 즉시 그 사실을 인지하고 신속하게 대처할 수가 있다. 특히 사용자IP를 커널 단계에서 확인시켜줌으로써 시스템의 수행률을 떨어뜨리지 않으면서도 사용자 구분이 이루어져 동시에 여러 명의 침입자가 발생하더라도 관리자는 시스템의 상황을 항상 정확하게 알 수가 있다.

57) 청구의 범위

청구항 1.

리눅스 시스템의 커널에서의 도1과 같은 침입을 탐지, 감시할 수 있는 제어 방식

청구항 2.

리눅스 시스템의 proc 파일시스템을 이용하여 커널이 데몬 프로그램에게 remote host IP 전달하는 방식

청구항 3.

리눅스 시스템의 데몬 프로그램이 침입을 판단하는 방식

청구항 4.

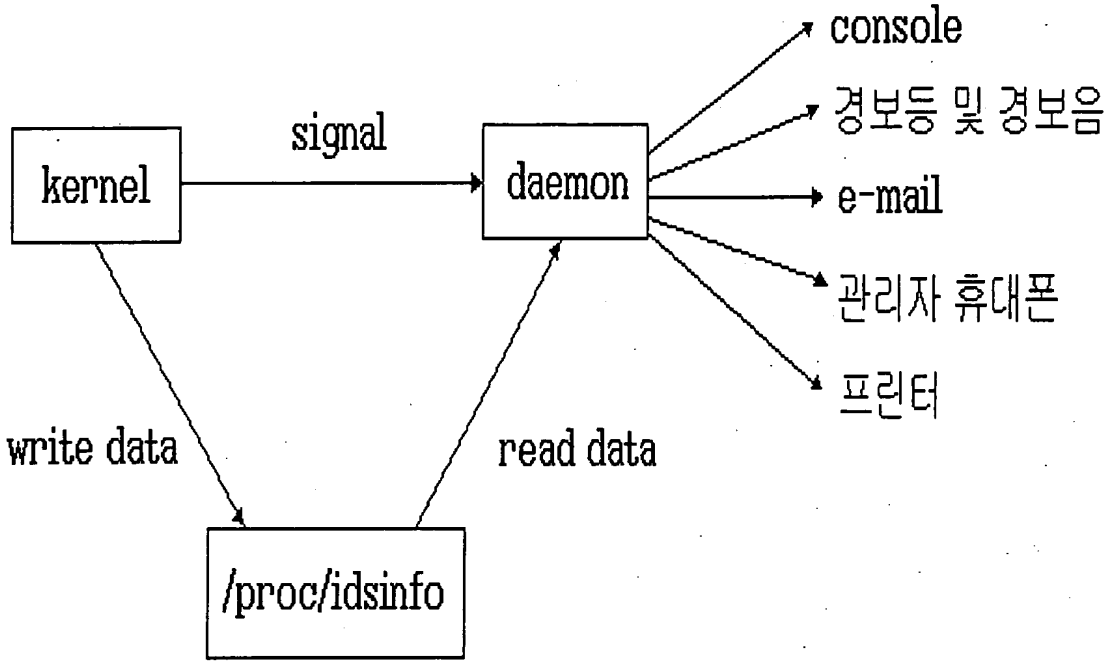
리눅스 시스템의 데몬 프로그램이 경보 발생시 서버에서 침입감시제어장치 [도3]를 제어하는 방식

청구항 5.

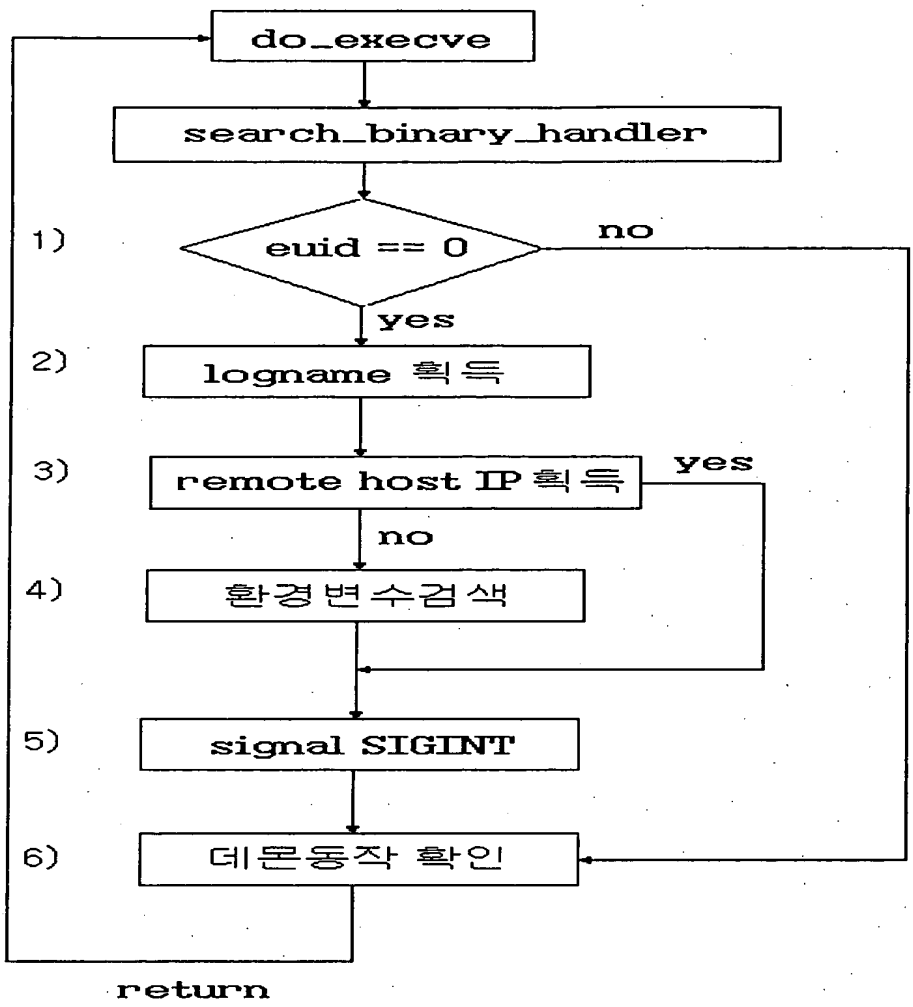
리눅스 시스템의 데몬 프로그램이 경보 발생시 서버에서 이메일 및 핸드폰으로 전송하는 방식

도면

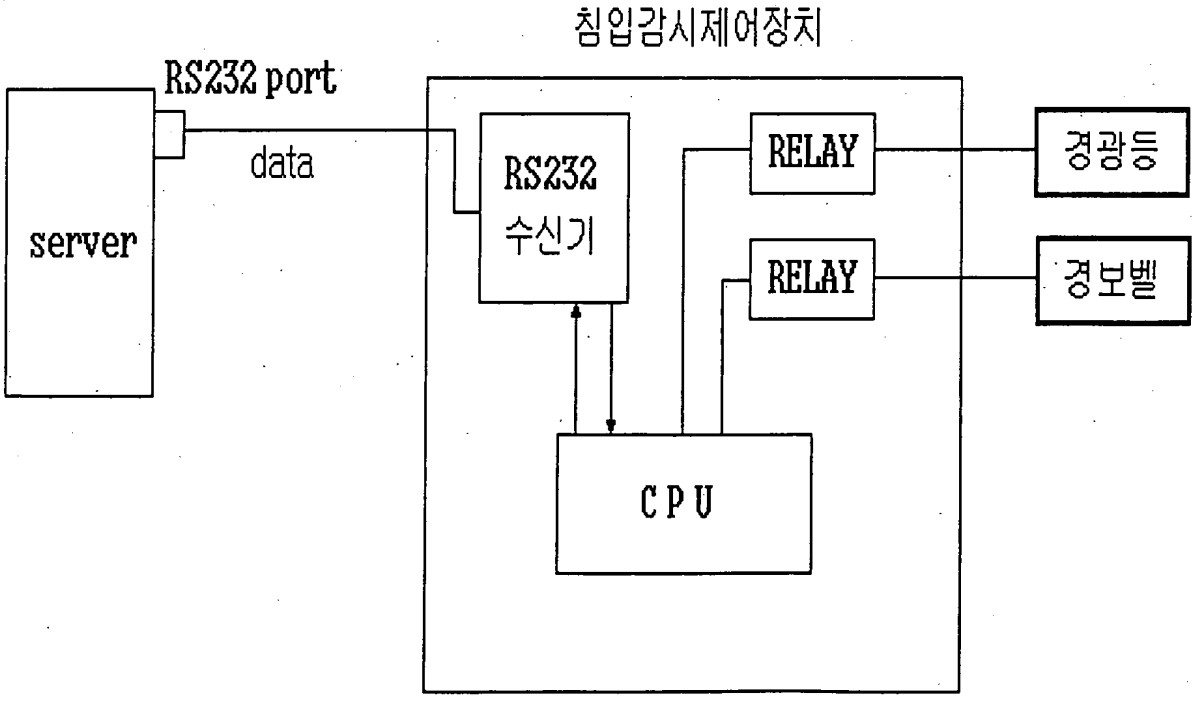
도면 1


kernel
signal
daemon
console
경보등 및 경보음
e-mail
관리자 휴대폰
프린터
write data
read data
/proc/idsinfo

도면 2


do_execve
search_binary_handler
1)
euid == 0
no
yes
2)
logname 획득
3)
remote host IP 획득
yes
no
4)
환경변수검색
5)
signal SIGINT
6)
데몬동작 확인
return

도면 3


침입감시제어장치
RS232 port
data
server
RS232
수신기
RELAY
RELAY
경광등
경보벨
CPU